SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN
Information Security Department

Circular No. 10 of 2025

Islamabad, May 12, 2025

Subject: SECP Cybersecurity Advisory

In light of the heightened geopolitical situation and the evolving cyber threat landscape, the Securities and Exchange Commission of Pakistan strongly advises all companies to adopt cybersecurity best practices in exercise of its powers conferred under section 40(B) of the Securities and Exchange Commission of Pakistan.

Potential Impacts

Failure to act on emerging cyber risks may result in:

a) **Operational Disruptions**: Cyberattacks may interrupt core functions including financial transactions and day to day operations.
b) **Data Breaches**: Exposure of data may lead to fraud and financial loss.
c) **Reputational Loss**: Loss of customer or investor trust.

(a) **Immediate Recommendations for Companies**

a) **Secure Access Controls:** Implement Multi-Factor Authentication (MFA) where ever applicable. Restrict application and user permissions strictly to only who need to have it.
b) **Build Awareness:** Train employees to recognize deceptive URLs, phishing attempts, and false communications that mimic official channels. Employees to avoid clicking on or circulating unverified links, particularly from messaging apps and social media platforms.
c) **Reducing Security Vulnerabilities**: Conduct vulnerability assessments and penetration testing of critical infrastructure, websites and patch identified security vulnerabilities.
d) **Network and Endpoint Security:** Deploy advanced antivirus tools and firewalls. Also, configure them as per manufacturer provided security guidelines. Also, keep anti-virus updated regularly.
e) **Build Readiness for Security Incidents:** Monitor network activities for abnormal behaviours. Maintain offline backups and validate data restoration regularly to recovery from incidents.
f) **Device and System Hardening:** Regularly patch systems and close unnecessary system services.
g) **Coordination and Incident Preparedness:** Establish internal incident response teams. Regularly consult National CERT (https://pkcert.gov.pk/) advisories and coordinate with relevant cybersecurity bodies for intelligence sharing and early threat detection.

All companies are urged to take immediate steps to implement the above suggested measures as per applicability, and maintain close liaison with SECP. Proactive measures are vital in safeguarding Pakistan's financial and information infrastructure.

Commissioner (ISD) –

Distribution:
All Companies